Release A CDR RID Report

Date Last Modified 9/28/95

Originator Gary Veum, Hal Folts **Phone No** 301-286-1073

Organization V0 networks, ESDIS

E Mail Address gary.veum@gsfc.nasa.gov

Document Overview of Release A SDPS and CSMS System Design Specification for the ECS Project.

Section 5.5.1 **Page** 5-29 **Figure Table** 5.5-1

RID ID CDR 75
Review SDPS/CSMS
Originator Ref DSNO 1
Priority 2

Category Name Hardware **Actionee** ECS

Sub Category

Subject FDDI switch limitations

Description of Problem or Suggestion:

The document states that the FDDI switch will be use for security as well as routing and switching. There is concern that the switch's performance will be impacted when many access lists are installed. This was discussed with an ECS network person, and they mentioned that 20-30 access lists have been installed without any impact. After discussing this with a MODNET/Nolan person, they mentioned that they use in the range of 200+ access lists on their firewall routers.

Originator's Recommendation

I believe an order of magnitude more access lists should be tested on this FDDI switch to prove that there is room for growth and expansion.

GSFC Response by: **GSFC Response Date**

HAIS Response by: D.Moore **HAIS Schedule** 9/20/95

HAIS R. E. D. Moore **HAIS Response Date** 9/22/95

The FDDI switch (Alantec PowerHub) is designed to handle filtering with minimal impact to performance. Tests conducted by HAIS involving 30 simultaneous filters resulted in negligible performance impact (e.g., performance drop was on the order of 2% average but was within the standard deviation of the measurements; performance actually increased with filters for many measurements).

Additionally, independent filtering tests of several routers (including Cisco, Wellfleet, Proteon, and NSC) were commissioned by the Department of Defense. The results of these tests showed that the "Alantec PowerHub demonstrated the best filtering performance of the routers tested." The tests involved creating varying numbers of different filters (at both the IP and TCP layers) on the routers and measuring the associated throughput. The number of filters applied ranged from 25 to 100. In all tests, the impact on performance for the Alantec was independent of the number of filters. In other words, the performance drop from the baseline non-filtering tests was the same for 25 filters up to 100 filters. Alantec has stated that they believe their performance with hold relatively constant independent of the number of filters applied and that they do not expect any additional degradation with increased filters.

ECS does not anticipate the need for a large amount of filters on a single switch for a variety of reasons. One reason is that the filtering scheme employed by ECS will be fairly simple, restricting access primarily on whether the traffic originates from within ECS or from outside ECS. This type of filtering can be accomplished with few filters, particularly considering that there are only eight ECS sites. Also, in Release B, ECS DAACs will generally employ separate user and processing networks, each generally controlled by its own router. This simplifies filtering considerably, because the user network is open to anyone and therefore will require only filters related to preventing certain TCP ports (such as for telnet or rlogin). Also, since the production network will not carry user traffic, its filtering scheme will be simplified as well. For these reasons, ECS does not anticipate requiring more than 50 filters in a given switch. If more than 100 filters are required, the tests discussed above suggest that the performance impact will be negligible.

Status **Closed** **Date Closed** **9/28/95** **Sponsor** **desJardins**

****** **Attachment if any** ******

Release A CDR RID Report